IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
Harrisonburg Division

CONSUMER FINANCIAL PROTECTION BUREAU; COMMONWEALTH OF MASSACHUSETTS; THE PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York; and COMMONWEALTH OF VIRGINIA, *EX REL.* MARK R. HERRING, ATTORNEY GENERAL, Plaintiffs, v. NEXUS SERVICES, INC.; LIBRE BY NEXUS, INC.; MICHEAL DONOVAN; RICHARD MOORE; and EVAN AJIN, Defendants.	Case No.: 5:21-cv-00016

STIPULATED ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

I. Purpose

This Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure and any other applicable orders and rules.

II. Preservation of ESI

The parties acknowledge that they have an obligation to take reasonable and proportional steps to preserve all potentially discoverable information in the party's possession, custody, or control. With respect to ESI preservation, the parties agree as follows:

A. All parties shall preserve all discoverable ESI in their possession, custody or control.

B. The parties have an ongoing duty to supplement discovery responses with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made, unless excluded under V below.

C. At a minimum, Defendants agree to preserve the following types of ESI. However, the below list is ***not*** exhaustive, and does not alter or limit any independent obligation Defendants have, under this order or otherwise, to verify that all potentially relevant ESI is being properly preserved.

1. Emails, including all email accounts over which Defendants communicate on topics related to the allegations in the Complaint. Defendants must preserve potentially relevant emails, regardless of their domain name or the main purpose of the account. For example, if employees use their personal email accounts to conduct business, those e-mails must be preserved. Because Mr. Donovan, Mr. Moore, and Mr. Ajin are named individually, Defendants agree to preserve all of their personal email accounts.

2. Text messages and instant messages, including but not limited to GroupMe and Slack, and instant messages such as SMS, WhatsApp, Telegram, and Signal, as well as social media direct and private messages. Again, Defendants must preserve all of these data sources if they contain information potentially relevant to the allegations in the Complaint, regardless of whether they are viewed as personal accounts. Because Mr. Donovan, Mr. Moore, and Mr.

Ajin are named individually, Defendants agree to preserve this information on their personal telephones, computers, and any relevant accounts.

3. Records and data from telephones used to communicate with consumers concerning topics alleged in the Complaint (again, regardless of whether the records and data are from personal phones).

4. Call recordings and voicemails (including, without limitation, both VoIP and mobile).

5. Capsule files (including metadata and logs).

6. Lightspeed files (including metadata and logs).

7. QuickBooks and other accounting records.

8. All electronic files, including those located on hard drives, shared drives, and cloud servers (again, regardless of whether such files are formally associated with business or personal computers or accounts).

D. If there are categories of ESI that a party believes in good faith need not be preserved, the parties will confer and reach agreement on those categories and maintain a written list of those categories.

III. Search Methodology and Criteria

A. Custodians. Prior to undertaking review and production of any ESI, the producing party must send to the receiving party a written list of custodians associated with each of the requesting party's requests, where individual employees are identifiable (as opposed to company records). The parties must meet and confer and reach agreement on which custodians' ESI is to be included in the search for each of the requesting party's requests.

B. Search Terms. To the extent the producing party intends to identify responsive documents through the use of search terms, the producing party and requesting party shall meet and confer regarding their use. The parties must submit to each other (a) a list of proposed terms and (b) a list of stop words and operators for the platform being used. The parties recognize that they may need to modify proposed search terms, whether submitted by the requesting or producing party, after receiving search term hit feedback if, for example, the terms generate a large amount of irrelevant or false positive results, and the parties agree to cooperate in good faith in negotiating and agreeing upon such modifications. Each party shall provide search term hit reports to the other, showing results of terms or queries including family (attachments) results and including results from applying deduplication. The parties agree that documents identified by search terms may be reviewed for privilege, confidentiality, relevance, or responsiveness prior to production.

C. Technology-Assisted Review. If either party employs any process that relies upon technology-assisted review, computer learning, analytics, or predictive coding to identify or eliminate documents, the parties must disclose the technology and process to be employed prior to beginning review of any documents. The party using technology assisted review must also provide (1) the selection method and total size of the initial review universe; (2) the selection method employed for training documents, confirming that subject-matter experts will be reviewing the seed set and training rounds; (3) criteria the party used to determine when the process is stopped (*e.g.*, if based on stability, the recall, precision, and confidence-level (or the equivalent) statistics); and (4) a validation process that allows the other party's representative to review statistically-significant random or selected samples of documents categorized as non-

responsive documents by the algorithm. If any party employs any process based on computer-assisted learning or any similar technology, it must ensure that the person responsible for coding the initial review set has substantial knowledge of the issues in this case.

IV. Production Format

A. Both parties shall produce all documents according to Attachments 1 and 2.

B. All ESI must be produced in electronic format and include "Bates" numbers or unique production numbers on each page. Plaintiffs will produce with letter prefixes designating the source (*e.g.*, "VAAG" for documents from the Virginia Attorney General's Office) followed by an 8-digit Bates number (e.g., VAAG01234567). Defendants will produce with the letter prefixes also designating the source (*e.g.*, "NEXUS" followed by an 8-digit Bates number, *e.g.*, NEXUS00000001, for documents produced by Nexus Services, Inc., DONOVAN000000001 for documents produced by Micheal Donovan, etc.).

C. Redactions. Any redacted material must be clearly labeled as having been redacted, and must include a notation with the basis for the redaction. Redactions are only permitted to withhold information protected by a recognized legal privilege or protection. Redactions for relevance are ***not*** permitted.

D. Families of Documents. The parties anticipate that they will encounter "families" of documents, which may include a "parent" email or document and one or more "child" attachments or embedded documents or documents accessible from an embedded link in the parent document. If any single document in a "family" is responsive, the parties agree that they must produce the entire family of documents. For example, if any one attachment to an email is responsive, then the cover email shall be produced for context,

regardless of the cover email's responsiveness. If the "child" document in a family is an embedded link, the parties agree to produce the version of the linked document that existed at the time of the creation of the parent document.

E. Deduplication. ESI will be deduplicated across all custodians (i.e., global deduplication) using generally accepted deduplication technology such as MD5 HASH. The metadata field with deduplication custodian information will be populated for custodians containing deduplication.

F. Media for Delivery of Production. ESI (including TIFF images and any native files) and scanned non-ESI documents in TIFF image format will be produced on a rolling basis to the requesting party on CD, DVD, hard drive or secure FTP. The case caption and the producing party shall be identified on each of such CD, DVD, or other media, along with the document production number range(s) corresponding to the contents of such CD, DVD, or other media and date of production.

V. Privileged and Protected Documents

For each document, tangible thing, or ESI withheld, in whole or in part, based on an asserted claim of privilege or protection, the party asserting the privilege must produce a privilege log.

For electronic documents, each party may opt at its own discretion to create privilege logs using one of the following methods. For paper documents, each party shall create privilege logs using the standard privilege log.

No matter the method of generating a privilege log that is chosen, the producing party must produce privilege logs on a rolling basis, within seven days of each document production, rather than at the end of discovery.

A. Automated Log. An automated privilege log will be generated from the following metadata fields, to the extent they exist, as electronic metadata associated with the original electronic documents.

1. SUBJECT
2. FILE NAME
3. AUTHOR
4. SENDER/FROM
5. RECIPIENTS/TO
6. CC
7. BCC
8. SENT DATE TIME
9. RECEIVED DATE TIME
10. FILE CREATED DATE TIME
11. FILE LAST MODIFIED DATE TIME

With respect to the SUBJECT OR FILENAME fields, the producing party may substitute a description of the communication where the content of these fields may reveal privileged information, but must indicate that the fields have been revised.

Parties shall include a field with information on privilege type, the basis for the privilege assertion, and whether the document has been produced with redactions.

Should the receiving party in good faith have reason to believe a particular entry on the Automated Log does not reflect a privileged document, it may request a Standard Log for that entry, to be produced within two weeks of the request, or within such other reasonable time as the parties may agree or the Court may order.

B. Standard Log. A standard privilege log will include these standard fields: author/sender/from; recipients/to; cc; bcc; date; privilege type, and a description sufficient to identify the subject of the document and the basis for the privilege assertion.

C. The privilege log fields for email strings will contain the information from the top email in the email string. Parties shall also populate a field with all other participants

identified on the face of the document not already captured in the top email of the email string. Other participants need only be identified for the email strings which are withheld as entirely privileged.

D. Parties need not note on a privilege log any documents exchanged solely among counsel or among counsel and employees or agents working on counsel's behalf in connection with this litigation such as investigators, paralegals, analysts, information technology and litigation support staff, or litigation support vendors.

E. The Plaintiffs need not note on a privilege log any communications or documents exchanged between each Plaintiff's respective office and/or other state or federal law enforcement agencies.

VI. Modification

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

DATED: 6/21/21

/s/ Hai Binh Nguyen
Attorneys for Plaintiff Consumer Financial Protection Bureau

DATED: 6/21/21

/s/ Jonathan Burke
Attorneys for Plaintiff Commonwealth of Massachusetts

DATED: 6/21/21

/s/ Stewart R. Dearing
Attorneys for Plaintiff People of the State of New York

DATED: 6/21/21

/s/ Erin E. Witte
Attorneys for Plaintiff Commonwealth of Virginia

DATED: 6/21/21

/s/ John M. Shoreman (with consent of counsel via email dated 6/21/21)
Attorneys for Defendants Nexus Services, Inc., Libre by Nexus, Inc., Micheal Donovan, Richard Moore, and Evan Ajin

IT IS SO ORDERED.

Entered: August 6, 2021.

/s/ Elizabeth K. Dillon
Elizabeth K. Dillon
United States District Judge

ATTACHMENT 1

Electronic Document Production Specifications

Unless otherwise specified and agreed to by the Plaintiffs, all responsive documents must be produced in LexisNexis® Concordance® format in accordance with the following instructions. Any questions regarding electronic document production should be directed to Plaintiffs.

1. Concordance Production Components. A Concordance production consists of the following component files, which must be produced in accordance with the specifications set forth below in Section 7.

   A. ***Metadata Load File.*** A delimited text file that lists in columnar format the required metadata for each produced document.

   B. ***Extracted or OCR Text Files.*** Document-level extracted text for each produced document or document-level optical character recognition ("OCR") text where extracted text is not available.

   C. ***Single-Page Image Files.*** Individual petrified page images of the produced documents in tagged image format ("TIF"), with page-level Bates number endorsements.

   D. ***Opticon Load File.*** A delimited text file that lists the single-page TIF files for each produced document and defines (i) the relative location of the TIF files on the production media and (ii) each document break.

   E. ***Native Files.*** Native format versions of non-printable or non–print friendly produced documents.

2. Production Folder Structure. The production must be organized according to the following standard folder structure:
   - data\ (contains production load files)
   - images\ (contains single-page TIF files, with subfolder organization)
     \0001, \0002, \0003…
   - native_files\ (contains native files, with subfolder organization)
     \0001, \0002, \0003…
   - text\ (contains text files, with subfolder organization)
     \0001, \0002, \0003…

3. De-Duplication. You must perform global de-duplication of stand-alone documents and email families.

4. Paper or Scanned Documents. Documents that exist only in paper format must be scanned to single-page TIF files and OCR'd. The resulting electronic files should be pursued in Concordance format pursuant to these instructions. You must contact Plaintiffs to discuss (i) any documents that cannot be scanned, and (ii) how information for scanned documents should be represented in the metadata load file.

5. Structured Data. Before producing structured data, including but not limited to relational databases, transactional data, and xml pages, you must first speak to Plaintiffs. Structured data is data that has a defined length and format and includes, but is not limited to, relational databases, graphical databases, JSON files, or xml/html pages.

A. Relational Databases

1. Database tables should be provided in CSV or other delimited machine-readable, non-proprietary format, with each table in a separate data file. The preferred delimiter is a vertical bar "|". If after speaking with Plaintiffs, it is determined that the data cannot be exported from a proprietary database, then the data can be produced in the proprietary format so long as the Plaintiffs are given sufficient access to that data.

2. Each database must have an accompanying Data Dictionary.

3. Dates and numbers must be clearly and consistently formatted and, where relevant, units of measure should be explained in the Data Dictionary.

4. Records must contain clear, unique identifiers, and the Data Dictionary must include explanations of how the files and records relate to one another.

5. Each data file must also have an accompanying summary file that provides total row counts for the entire dataset and total row counts.

B. Compression

1. If Documents are provided in a compressed archive, only standard lossless compression methods (e.g., gzip, bzip2, and ZIP) shall be used. Media files should be provided in their original file format, with metadata preserved and no additional lossy encoding applied.

6. Media and Encryption. All documents must be produced on CD, DVD, or hard-drive media. After consultation with the Plaintiffs, Documents may also be produced over a secure file transfer protocol (FTP), a pre-approved cloud-based platform (e.g. Amazon Web Services S3 bucket), or the New York Attorney General's cloud platform OAGCloud. All production media must be protected with a strong, randomly-generated password containing at least 16 alphanumeric characters and encrypted using Advanced Encryption Standard with 256-bit key length (AES-256). Passwords for electronic documents, files, compressed archives and encrypted media must be provided separately from the media.

7. Production File Requirements.

A. ***Metadata Load File***

- Required file format:
  - ASCII or UTF-8
  - Windows formatted CR + LF end of line characters, including full CR + LF on last record in file.
  - .dat file extension
  - Field delimiter: (ASCII decimal character 20)
  - Text Qualifier: þ (ASCII decimal character 254). Date and pure numeric value fields do not require qualifiers.
  - Multiple value field delimiter: ; (ASCII decimal character 59)
- The first line of the metadata load file must list all included fields. All required fields are listed in Attachment 2.
- Fields with no values must be represented by empty columns maintaining delimiters and qualifiers.
- ***Note:*** All documents must have page-level Bates numbering (except documents produced only in native format, which must be assigned a document-level Bates number). The metadata load file must list the beginning and ending Bates numbers (BEGDOC and ENDDOC) for each document. For document families, including but not limited to emails and attachments, compound documents, and uncompressed file containers, the metadata load file must also list the Bates range of the entire document family (ATTACHRANGE), beginning with the first Bates number (BEGDOC) of the "parent" document and ending with the last Bates number (ENDDOC) assigned to the last "child" in the document family.
- Date and Time metadata must be provided in separate columns.
- Accepted date formats:
  - mm/dd/yyyy
  - yyyy/mm/dd
  - yyyymmdd
- Accepted time formats:
  - hh:mm:ss (if not in 24-hour format, you must indicate am/pm)
  - hh:mm:ss:mmm

B. ***Extracted or OCR Text Files***

- You must produce individual document-level text files containing the full extracted text for each produced document.
- When extracted text is not available (for instance, for image-only documents) you must provide individual document-level text files containing the document's full OCR text.
- The filename for each text file must match the document's beginning Bates number (BEGDOC) listed in the metadata load file.
- Text files must be divided into subfolders containing no more than 500 to 1000 files.

C. ***Single-Page Image Files (Petrified Page Images)***

- Where possible, all produced documents must be converted into single-page tagged image format ("TIF") files. See Section 7.E below for instructions on producing native versions of documents you are unable to convert.
- Image documents that exist only in non-TIF formats must be converted into TIF files. The original image format must be produced as a native file as described in Section 7.E below.
- For documents produced only in native format, you must provide a TIF placeholder that states "Document produced only in native format."
- Each single-page TIF file must be endorsed with a unique Bates number.
- The filename for each single-page TIF file must match the unique page-level Bates number (or document-level Bates number for documents produced only in native format).
- Required image file format:
  - CCITT Group 4 compression
  - 2-Bit black and white
  - 300 dpi
  - Either .tif or .tiff file extension.
- TIF files must be divided into subfolders containing no more than 500 to 1000 files. Where possible documents should not span multiple subfolders.

D. ***Opticon Load File***

- Required file format:
  - ASCII
  - Windows formatted CR + LF end of line characters
  - Field delimiter: , (ASCII decimal character 44)
  - No Text Qualifier
  - .opt file extension
- The comma-delimited Opticon load file must contain the following seven fields (as indicated below, values for certain fields may be left blank):
  - ALIAS or IMAGEKEY – the unique Bates number assigned to each page of the production.
  - VOLUME – this value is optional and may be left blank.
  - RELATIVE PATH – the filepath to each single-page image file on the production media.
  - DOCUMENT BREAK – defines the first page of a document. The only possible values for this field are "Y" or blank.
  - FOLDER BREAK – defines the first page of a folder. The only possible values for this field are "Y" or blank.
  - BOX BREAK – defines the first page of a box. The only possible values for this field are "Y" or blank.
  - PAGE COUNT – this value is optional and may be left blank.
- ***Example*:**

ABC00001,,IMAGES\0001\ABC00001.tif,Y,,,2
ABC00002,,IMAGES\0001\ABC00002.tif,,,,
ABC00003,,IMAGES\0002\ABC00003.tif,Y,,,1
ABC00004,,IMAGES\0002\ABC00004.tif,Y,,,1

E. ***Native Files***

- Non-printable or non–print friendly documents (including but not limited to spreadsheets, audio files, video files and documents for which color has significance to document fidelity) must be produced in their native format.
- The filename of each native file must match the document's beginning Bates number (BEGDOC) in the metadata load file and retain the original file extension.
- For documents produced only in native format, you must assign a single document-level Bates number and provide an image file placeholder that states "Document produced only in native format."
- The relative paths to all native files on the production media must be listed in the NATIVEFILE field of the metadata load file.
- Native files that are password-protected must be decrypted prior to conversion and produced in decrypted form. In cases where this cannot be achieved the document's password must be listed in the metadata load file. The password should be placed in the COMMENTS field with the format Password: <PASSWORD>.
- You may be required to supply a software license for proprietary documents produced only in native format.

ATTACHMENT 2
Required Fields for Metadata Load File

FIELD NAME	FIELD DESCRIPTION	FIELD VALUE EXAMPLE[1]
DOCID	Unique document reference (can be used for de-duplication).	ABC0001 or ###.######.###
BEGDOC	Bates number assigned to the first page of the document.	ABC0001
ENDDOC	Bates number assigned to the last page of the document.	ABC0002
BEGATTACH	Bates number assigned to the first page of the parent document in a document family (*i.e.*, should be the same as BEGDOC of the parent document, or PARENTDOC).	ABC0001
ENDATTACH	Bates number assigned to the last page of the last child document in a family (*i.e.*, should be the same as ENDDOC of the last child document).	ABC0008
ATTACHRANGE	Bates range of entire document family.	ABC0001 - ABC0008
PARENTDOC	BEGDOC of parent document.	ABC0001
CHILDDOCS	List of BEGDOCs of all child documents, delimited by ";" when field has multiple values.	ABC0002; ABC0003; ABC0004...
DOCREQ	List of particular Requests for Documents to be Produced	1; 2; 3 . . .
INTERROG	List of particular Interrogatories	1; 2; 3 . . .
COMMENTS	Additional document comments, such as passwords for encrypted files.	
NATIVEFILE	Relative file path of the native file on the production media.	.\Native_File\Folder\... \BEGDOC.ext

[1] Examples represent possible values and not required format unless the field format is specified in Attachment 1.

SOURCE	For scanned paper records this should be a description of the physical location of the original paper record. For loose electronic files this should be the name of the file server or workstation where the files were gathered.	Company Name, Department Name, Location, Box Number...
CUSTODIAN	Owner of the document or file.	Firstname Lastname, Lastname, Firstname, User Name; Company Name, Department Name...
FROM	Sender of the email.	Firstname Lastname < FLastname @domain >
TO	All to: members or recipients, delimited by ";" when field has multiple values.	Firstname Lastname < FLastname @domain >; Firstname Lastname < FLastname @domain >; ...
CC	All cc: members, delimited by ";" when field has multiple values.	Firstname Lastname < FLastname @domain >; Firstname Lastname < FLastname @domain >; ...
BCC	All bcc: members, delimited by ";" when field has multiple values	Firstname Lastname < FLastname @domain >; Firstname Lastname < FLastname @domain >; ...
SUBJECT	Subject line of the email.	
DATERCVD	Date that an email was received.	mm/dd/yyyy, yyyy/mm/dd, or yyyymmdd
TIMERCVD	Time that an email was received.	hh:mm:ss AM/PM or hh:mm:ss
DATESENT	Date that an email was sent.	mm/dd/yyyy, yyyy/mm/dd, or yyyymmdd
TIMESENT	Time that an email was sent.	hh:mm:ss AM/PM or hh:mm:ss

CALBEGDATE	Date that a meeting begins.	mm/dd/yyyy, yyyy/mm/dd, or yyyymmdd
CALBEGTIME	Time that a meeting begins.	hh:mm:ss AM/PM or hh:mm:ss
CALENDDATE	Date that a meeting ends.	mm/dd/yyyy, yyyy/mm/dd, or yyyymmdd
CALENDTIME	Time that a meeting ends.	hh:mm:ss AM/PM or hh:mm:ss
CALENDARDUR	Duration of a meeting in hours.	0.75, 1.5...
ATTACHMENTS	List of filenames of all attachments, delimited by ";" when field has multiple values.	AttachmentFileName.; AttachmentFileName.docx; AttachmentFileName.pdf;...
NUMATTACH	Number of attachments.	1, 2, 3, 4....
RECORDTYPE	General type of record.	IMAGE; LOOSE E-MAIL; E-MAIL; E-DOC; IMAGE ATTACHMENT; LOOSE E-MAIL ATTACHMENT; E-MAIL ATTACHMENT; E-DOC ATTACHMENT
FOLDERLOC	Original folder path of the produced document.	Drive:\Folder\...\...\
FILENAME	Original filename of the produced document.	Filename.ext
DOCEXT	Original file extension.	html, xls, pdf
DOCTYPE	Name of the program that created the produced document.	Adobe Acrobat, Microsoft Word, Microsoft Excel, Corel WordPerfect...
TITLE	Document title (if entered).	
AUTHOR	Name of the document author.	Firstname Lastname; Lastname, First Name; FLastname
REVISION	Number of revisions to a document.	18

DATECREATED	Date that a document was created.	mm/dd/yyyy, yyyy/mm/dd, or yyyymmdd
TIMECREATED	Time that a document was created.	hh:mm:ss AM/PM or hh:mm:ss
DATEMOD	Date that a document was last modified.	mm/dd/yyyy, yyyy/mm/dd, or yyyymmdd
TIMEMOD	Time that a document was last modified.	hh:mm:ss AM/PM or hh:mm:ss
FILESIZE	Original file size in bytes.	128, 512, 1024…
PGCOUNT	Number of pages per document.	1, 2, 10, 100…
IMPORTANCE	Email priority level if set.	Low, Normal, High
TIFFSTATUS	Generated by the Law Pre-discovery production tool (leave blank if inapplicable).	Y, C, E, W, N, P
DUPSTATUS	Generated by the Law Pre-discovery production tool (leave blank if inapplicable).	P
MD5HASH	MD5 hash value computed from native file (a/k/a file fingerprint).	BC1C5CA6C1945179FEE144F25F51087B
SHA1HASH	SHA1 hash value	B68F4F57223CA7DA3584BAD7ECF111B8044F8631
MSGINDEX	Email message ID	